AFRL-RZ-WP-TR-2012-0105

META II: FORMAL CO-VERIFICATION OF CORRECTNESS OF LARGE-SCALE CYBER-PHYSICAL SYSTEMS DURING DESIGN (Mod 0006)

Volume 2

Walter Johnson

Palo Alto Research Center

MARCH 2012
Final Report

Approved for public release; distribution unlimited.

See additional restrictions described on inside pages

STINFO COPY

AIR FORCE RESEARCH LABORATORY
PROPULSION DIRECTORATE
WRIGHT-PATTERSON AIR FORCE BASE, OH 45433-7251
AIR FORCE MATERIEL COMMAND
UNITED STATES AIR FORCE

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the USAF 88th Air Base Wing (88 ABW) Public Affairs Office (PAO) and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RZ-WP-TR-2012-0105 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH THE ASSIGNED DISTRIBUTION STATEMENT.

*//Signature//	//Signature//
DOUGLAS R. RANEY	JACK VONDRELL
Project Engineer	Branch Chief
Mechanical Energy Conversion Branch	Mechanical Energy Conversion Branch
Energy/Power/Thermal Division	Energy/Power/Thermal Division
Propulsion Directorate	Propulsion Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

*Disseminated copies will show "//Signature//" stamped or typed above the signature blocks.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS**.

1. REPORT DATE ***(DD-MM-YY)***	**2. REPORT TYPE**	**3. DATES COVERED** ***(From - To)***
March 2012	Final	10 November 2011 – 29 February 2012

4. TITLE AND SUBTITLE
META II: FORMAL CO-VERIFICATION OF CORRECTNESS OF LARGE-SCALE CYBER-PHYSICAL SYSTEMS DURING DESIGN (Mod 0006)
Volume 2

5a. CONTRACT NUMBER
FA8650-10-C-7079

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
62303E

6. AUTHOR(S)
Walter Johnson

5d. PROJECT NUMBER
DM30

5e. TASK NUMBER
01

5f. WORK UNIT NUMBER
DM300108

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Palo Alto Research Center
3333 Coyote Hill Road
Palo Alto, CA 94304

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory
Propulsion Directorate
Wright-Patterson Air Force Base, OH 45433-7251
Air Force Materiel Command
United States Air Force

10. SPONSORING/MONITORING AGENCY ACRONYM(S)
AFRL/RZPG

11. SPONSORING/MONITORING AGENCY REPORT NUMBER(S)
AFRL-RZ-WP-TR-2012-0105

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES
Report contains color. PA Case Number: 88ABW-2012-1688; Clearance Date: 23 Mar 2012.
See also Volume 1, AFRL-RZ-WP-TR-2011-2110.

14. ABSTRACT
Design and development of complex vehicle and weapon systems remains a substantial challenge to the DoD. A robust, scalable, and affordable tool chain based on the technologies developed under the META program would provide the DoD community with a capability that will enable correct-by-construction design of such systems. The ultimate goal is to achieve DARPA's vision of 5x compression in the time it takes to deploy such systems. The proposed work facilitates the development of such a tool chain by studying approaches for commercialization and long- term viability of the tool chain.

15. SUBJECT TERMS
design, design tools, model-based design, verification, certification

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT:**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** (Monitor)
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Douglas R. Raney
Unclassified	Unclassified	Unclassified	SAR	28	**19b. TELEPHONE NUMBER** *(Include Area Code)* N/A

TABLE OF CONTENTS

Approved for public release; distribution unlimited.

List of Figures

List of Tables

Approved for public release; distribution unlimited.

1.0 SUMMARY

The complexity of modern defense systems is growing constantly. New technologies create opportunities for higher levels of integration. Modern systems such as air and ground vehicles contain a larger number of components that interact with each other in non-linear and often unpredictable ways. Unintended interactions lead to unexpected behaviors and consequences, some of which have proven to be catastrophic. A key technical challenge in developing such complex systems is to ensure that catastrophic subsystem and component interactions are well understood and contained prior to full-scale development.

To address these challenges, The Defense Advanced Research Projects Agency (DARPA) is investing in novel methods for design and verification of complex systems. The META program (META not an acronym but is typically spelled using all capital letters by DARPA) is specifically aimed at compressing the product development and deployment timeline of complex defense systems through model-based design and manufacturing. Using the META design paradigm, different component model libraries can be used to instantiate, analyze, and verify a system design independent of its physical manifestation. The goal is to establish a "correct-by-construction" design prior to detailed design and prototyping.

During the 12-month base period of the META-II program, a team led by the PARC (Palo Alto Research Center) team has developed a model-based system-engineering framework that enables architectural analysis of complex systems during the conceptual design phase. Using this framework, design teams are able to systematically explore architectural design decisions during the early stage of system development prior to the selection of specific components [1]. The analysis performed at this earliest stage of design facilitates the development of more robust and reliable system architectures. A final report summarizing this work was submitted at the end of the original period of performance.

The META-II contract was extended effective November 10, 2011 to study the commercial viability of the design tool chain being developed under the META and META-II programs. This final report provides a summary of the short-term study conducted by the PARC team on the potential of the META tool chain for technology transition and commercialization.

Approved for public release; distribution unlimited.

2.0 INTRODUCTION

The complexity of modern defense systems is growing constantly. New technologies create opportunities for higher levels of integration. Modern systems such as air and ground vehicles contain a larger number of components that interact with each other in non-linear and often unpredictable ways. Unintended interactions lead to unexpected behaviors and consequences, some of which have proven to be catastrophic. A key technical challenge in developing such complex systems is to ensure that catastrophic subsystem and component interactions are well understood and contained prior to full-scale development.

To address these challenges, DARPA is investing in novel methods for design and verification of complex systems. The META program is specifically aimed at compressing the product development and deployment timeline of complex defense systems through model-based design and manufacturing. Using the META design paradigm, different component model libraries can be used to instantiate, analyze, and verify a system design independent of its physical manifestation. The goal is to establish a "correct-by-construction" design prior to detailed design and prototyping.

During the 12-month base period of the META-II program, a team led by PARC (Palo Alto Research Center) has developed a model-based system-engineering framework that enables architectural analysis of complex systems during the conceptual design phase. Using this framework, design teams are able to systematically explore architectural design decisions during the early stage of system development prior to the selection of specific components. The analysis performed at this earliest stage of design facilitates the development of more robust and reliable system architectures.

The META-II contract was extended effective November 10, 2011 to study the commercial viability of the design tool chain being developed under the META and META-II programs. The goals of the commercialization and design study include:

- Study of the market for design tools, identification of the gaps, and assessment of the market demand for innovative capabilities being developed under the META and META-II programs.

- Investigation of the needs of designers of complex cyber-electro- mechanical systems.

- Development of requirements for a mass-market design tool chain that meets the requirements of the FANG performer base.

- Development of a roadmap and timeline for META tool chain commercialization in order to meet the needs of the DARPA AVM program.

Approved for public release; distribution unlimited.

- Development of a high-level architecture for a scalable, robust, and affordable tool chain for the design of cyber-electro-mechanical systems based on META R&T.

- A study of the provenance of each tool to be integrated in the tool chain.

2.1 Impact Statement

We believe that a systematic approach that identifies design defects, uncertainty, and unforeseen fault propagation effects during the early design process will compress DDTE schedules significantly. Desired improvements of >5x are within reach if the methods developed under the META program are widely adopted in the defense community. Much of the complexity and cost of verification is mandated through complex policies such DO-254, DO-178B, and NASA's NPR 8705.2B (Human Rating Requirements). We envision that a successful conclusion to these programs would yield revolutionary new methods, tools, and processes that will help refine the rigid procedural requirements that impose substantial delays and cost overruns on every major aerospace program today.

We also believe that the accomplishments made during the META and META-II R&T programs need to be further matured and commercialized in order to make a significant impact in the compression of DDTE schedules. The ultimate impact of this achievement will be early elimination of design flaws, reduced need for hardware-in-the-loop testing, and compressed design cycle times.

Approved for public release; distribution unlimited.

3.0 METHODS, ASSUMPTIONS, AND PROCEDURES

3.1 Market Survey

Through a subcontract with RedHouse Consulting, PARC investigated the market for design tools, identified the gaps, and assessed the market demand for innovative capabilities being developed under the META and META-II programs. RedHouse conducted interviews with product designers and other end users to document capabilities that are missing in existing tool suites. RedHouse also identified several distinct market segments for design tools; studied the market penetration of end-to-end design tool chains in these market segments; and attempted to quantify the market size for a new tool chain based on the META R&T activities. RedHouse studied the business models for existing tool chains as well as standalone tools currently available for the design of cyber-electro-mechanical systems. RedHouse identified multiple potential business models to address the issue of long-term viability and self-sustenance of the new tool chain in a competitive marketplace. Finally, RedHouse assessed the viability of each market segment as an initial target market for a commercial tool chain based on open source deliverables of the META/META-II programs. The primary deliverable was a Market Survey with was delivered to the Government in December 2011.

3.2 User Needs

The PARC team investigated the needs of designers of complex cyber-electro-mechanical systems. The user needs study focused on key vertical markets for design tools including automotive, biomedical devices, aerospace, and consumer electronics. In addition, the team interviewed several industry analysts. The primary deliverables were a Market Requirements Document (MRD) and the Ethnographic Study Report.

3.3 Tool Chain Requirements

The PARC team developed the requirements for a mass-market design tool chain that met the requirements of the FANG performer base. The requirements included user interaction needs, functional needs, performance needs, external interfaces (e.g., with existing tool chains), and security requirements. The primary deliverables were a Product Requirements Document (PRD) and formal specifications for the tool chain in UML format.

3.4 Commercialization Approach

The PARC team outlined plan and roadmap for META tool chain commercialization in order to meet the needs of the DARPA AVM program. The primary deliverable was a commercialization plan.

3.5 Architecture Design

The PARC team developed a high-level architecture for a scalable, robust, and affordable tool chain for the design of cyber-electro-mechanical systems based on META R&T. Specific requirements for this architecture include:

- Zero or limited installation effort
- No third party licensing requirements for users

Approved for public release; distribution unlimited.

- Potential to scale to thousands of simultaneous users
- Cloud computing capabilities for increased speed and response time
- End-to-end design platform with all major design functions provided in one integrated tool chain
- Integration with leading product lifecycle management (PLM) and computer- aided engineering (CAE) tools (including popular solid modeling, mathematical solvers, finite element analysis, multi-physics analysis. etc.)
- Integration with the DARPA-sponsored VehicleForge.mil model libraries and C2M2L component libraries.

The architecture specification includes tool capabilities, input/output requirements (e.g., supported modeling languages), tool provenance, and licensing requirements. The primary deliverable is an Architecture Design Specification that includes block diagrams (modules, function level etc.) as well as a formal specification in UML format.

3.6 Intellectual Property Analysis

The PARC team studied the provenance of each tool to be integrated in the tool chain. Specifically, DARPA is interested in understanding the IP rights and restrictions applicable to each candidate implementation for each tool required in the architecture. This analysis includes licensing requirements, if any, and a make-or-buy recommendation for each element in the tool chain. The primary deliverable is an Intellectual Property Report.

Approved for public release; distribution unlimited.

4.0 RESULTS AND DISCUSSIONS

4.1 Market Survey

Design tools developed under the META and META-II programs fall under the category of Product Lifecycle Management (PLM) tools. The PLM term came into use about 15 years ago to categorize software used by companies to manage the information associated with developing a product and transitioning it to manufacturing. A definition of PLM is as follows:

"A set of business solutions in support of the collaborative creation, management, dissemination, and use of product definition information across the extended enterprise, and spanning from product concept to end of life."

PLM software is generally used by companies developing physical or hardware products. A different class of software, Application Lifecycle Management (ALM) is used by companies developing software products. In the last decade, PLM software has been extended for use by process industries as well as by discrete manufacturers.

Industry analyst firm CIMData breaks down the PLM market as follows:

A. Collaborative Product Data Management (PDM)
B. Digital Manufacturing
C. Tools
    1. Mechanical Computer-Aided Design (MCAD)
    2. Electronic Design Automation (EDA)
    3. Simulation/Analysis
    4. Architecture, Engineering, Construction (AEC)
    5. Computer-Aided Software Engineering (CASE)

Total revenues in the PLM market reached $25.8B in 2010, broken down as shown in Figure 1.

Approved for public release; distribution unlimited.

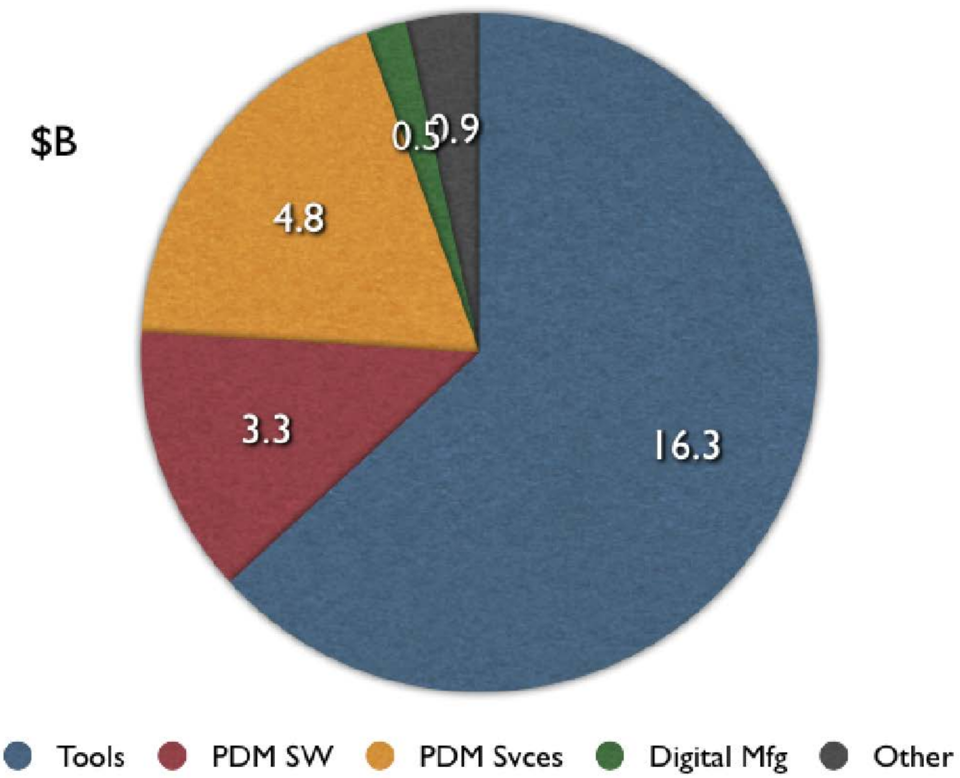

Figure 1. Global PLM Market Size (2010)

The META/META-II commercialization work falls in the Tools segment. The CAD and EDA markets are relatively mature, but two key trends are driving the market:

- Increasing penetration of “low-end” CAD tools into the “high end”. Traditionally, analysts have differentiated between 2D and 3D CAD, but now the low-end tools are 3D and increasingly able to do tasks once reserved for high-end CAD. The price differences are considerable, with traditional high end CAD often over $10K per seat, and low end CAD well under $5K per seat. AutoCAD (AutoDesk) and SolidWorks (Dassault) seem best positioned to capitalize on this trend.
- Convergence of mechanical, electrical, and control software design, often referred to as “mechatronics”. As traditionally mechanical products such as cars, refrigerators, etc. incorporate more electronics and software, designers are seeking tools that combine the disciplines rather than doing separate design and analysis for each. Mechatronics is receiving a lot of attention and discussion, but there are few commercial offerings outside of academia. The CAD vendors are generally perceived to be slow at coming up with solutions, and some feel that EDA vendors may in fact get there first.

The tools market is further subdivided into several categories as indicated in Figure 2.

Approved for public release; distribution unlimited.

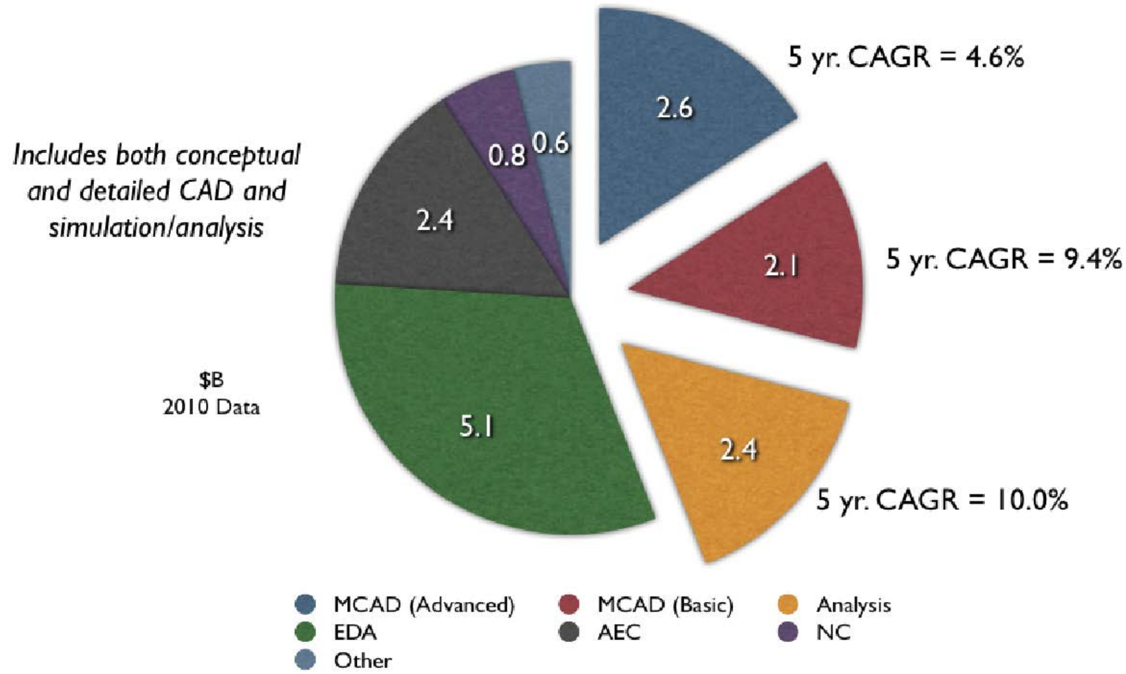

Figure 2. Global Market Size for the Tools Segment (2010)

As we can see, the traditional high-end CAD market is mature and not expected to grow that rapidly over the next five years. Rather, the low-end CAD tools are expected to grow rapidly as they add capabilities. The simulation and analysis market is expected to grow at a 10% CAGR over five years. META tools fall under the $2.4B market in Simulation and Analysis. This category includes conceptual/early design and analysis tools as well as detailed analysis tools such as structural, thermal, electromagnetic, noise, vibration analysis, etc.

We see some obstacles to the rapid adoption of model-based design tools. First, the discipline of system engineering is not well understood outside of Aerospace and Defense (A&D), Automotive, and some academic settings. Secondly, the fragmentation of engineering disciplines among mechanical, electrical, software, and the resulting fragmentation of data, will make implementing system engineering that much harder. Finally, we heard from nearly every company about the lack of good modelers and the inability to hire top graduates because of U.S. visa restrictions.

Companies will adopt model-based design and verification tools when they have strong business reasons to do so. The alternative to model-based design and verification is multiple prototyping. Companies will only shift from this when prototyping is either too expensive (as, for example, in A&D) or too time-consuming for meeting market windows (as, for example, in Automotive). Model-based design and verification will also require a different way of thinking within R&D organizations, which will occur only when there is sufficient understanding of the costs and benefits.

Approved for public release; distribution unlimited.

4.2 User Needs

We identified target interview candidates as exhibiting the following characteristics:

- Complex electromechanical design challenges
- Perceives value in early model-based design to shorten time to market and reduce prototyping
- Compliance or certification requirements a plus
- Able/willing to shift from current design tools
- Able/willing to use cloud-based services

We identified Automotive, High End Medical Devices, and Semiconductor Manufacturing Equipment companies as fitting this profile. We also felt that it was useful to interview other high tech companies not in medical devices. After some initial conversations with people in semiconductor manufacturing equipment companies, we decided to drop that sector due to a lack of real innovation focus.

Table 1 lists the companies that we interviewed during this project. In addition, we interviewed four industry experts.

Automotive	Medical Devices	High Tech Other	System Integrators
GM	Intuitive Surgical	Kaleidescape	Accenture
Tesla	Hansen Medical	NeoPhotonics	Kalypso
Magna E-Cars	Covidien	Xerox	PRTM
	Medtronic	Logitech	

Table 1. List of user interviews conducted by our team

Based on the initial market research, we developed several assumptions that we wanted to test in the interviews. A summary of our assumptions and findings after completing the interviews is listed below.

1. **Companies in target segments are spending 3-5% of R&D spending on tools and PDM.**

Where we could get the data, it was 3-4% of R&D spending. Thus, we feel reasonably confident about our assumption on the percentage of R&D spending that companies allocate to PLM.

Approved for public release; distribution unlimited.

2. **Incumbent tools are not well liked, but may be "sticky."**

Tools are sticky because of high learning curves as long as several months. Once a company has made the investment, they will not displace the tool easily. This means that META tools need to be an add-on to, not a replacement for, current tools - at least initially.

3. **Opportunities exist in conceptual modeling, especially for the combination of mechanical and control software.**

Yes, but the discipline is not well understood today. The value proposition is strongest in A&D and Automotive because requirements are better defined, and because systems engineering has been practiced there for decades. But in our discussions with medical device companies, we discovered little awareness of and investment in systems engineering or model-based design. We expect that the same is true of the Industrial Equipment sector.

4. **Some collaboration software is needed to make the tool chain attractive, but how much?**

Sharing and reuse of models and components (subsystems) through some sort of library will be an important capability. Some companies are thinking about this already. Linking to Requirements Management tools such as DOORS may be important, in order to allow designers to check simulation results against requirements.

5. **Data management in conceptual design phases is disorganized, primarily using "free" Microsoft tools and manual effort.**

We did find this to be true, but nobody seems to be concerned about it. This may be because design groups are typically fragmented into Mechanical Engineering, Electrical Engineering, Firmware Engineering, and so forth. This fragmentation represents an obstacle to "mechatronics" and system engineering because data is in separate formats and databases, and hard to combine.

6. **Willingness to use cloud-based design tools and collaboration is increasing.**

There was a real split here between large and small companies. Only the small companies seemed comfortable about adopting cloud-based tools. Larger companies would not even entertain the discussion, and will likely use only private clouds. They have great concern about security and loss of intellectual property. Whether their data is truly more secure inside their firewall - and most of the analysts we talked to doubted it - that is how they perceive it. This attitude will take several years to break down in Automotive and A&D. High tech companies in general are more savvy about the cloud and data security, and are likely to adopt cloud-based products sooner.

We also had some interesting findings that were not anticipated before conducting the interviews:

- PLM Vendors - Siemens TeamCenter and Dassault Enovia were the dominant vendors in the automotive sector. These companies tend to become one-stop shops, so that Siemens or Dassault are used not only for PDM but for all CAD and for CAE where applicable. In the high tech and medical device sectors, Agile was the dominant PDM vendor, and among the smaller companies Arena Solutions was known and being considered. We were surprised at the dominance of Agile and the awareness of Arena, despite being such a small company.

Approved for public release; distribution unlimited.

- CAD Vendors - SolidWorks was very prominent among the companies we talked to, albeit less so in the automotive sector. A few companies talked about replacing more expensive CAD tools, especially Pro-E (PTC), with SolidWorks. This illustrates a trend of low-end CAD tools moving up the value chain and displacing the traditional higher-end CAD tools.
- Licensing models - The predominant models of named or floating seat-based licenses used by PLM and CAD companies are frustrating to the users. This suggests that a cloud-based pay-per-use model for PLM could disrupt the current model. Arena Solutions is doing this for PDM; Altair and AutoDesk are experimenting with this model for CAE and CAD.

4.3 Tool Chain Requirements

PARC identified CyDesign Labs, a small business, as a partner to develop the META tool chain requirements. As a subcontractor to PARC, CyDesign Labs developed and delivered a Product Requirements Document (PRD) and a Tool Chain Formal Specifications document.

The PRD covers CyDesign Studio, a commercial design tool chain based on META tools. The Tool Chain Formal Specifications document covers the various elements of the tool chain and their interdependencies. A summary of the approach is provided below.

The purpose of CyDesign Studio is to provide a mass-market tool suite for model-based design of complex cyber-electromechanical systems. CyDesign Studio will address trade space exploration and requirements verification using system models composed from component model libraries. CyDesign Studio will enable verification of system models with respect to requirements, and allow designers to engage stakeholders in understanding important design tradeoffs. Major benefits of the product are: 1) more thorough exploration of the design trade space; 2) early verification of major system requirements using models; 3) schedule and cost savings through elimination of design-build-test cycles.

The CyDesign platform will be built from the ground up to run in the cloud. As such, it will be architected to be highly scalable and available using current best practices in the areas of network, database, storage, and virtualization. It will be virtualization agnostic, however, so it will run in a variety of cloud based offerings including Amazon EC2, Rackspace Cloud Services, and others to be determined based on market demand. CyDesign Studio will support both public implementations as well as private implementations. The latter would only be available to users within a single organization or associated with a specific design effort.

In addition to the cloud offerings, CyDesign Studio will support a more traditional software deployment model where by the entire platform can be installed onsite. That latter requirement will satisfy the needs of customers who have more strict security requirements or just wish to have greater control over their proprietary designs.

Regardless of how the CyDesign Studio platform is deployed, it will exploit the advantages of virtualization for on demand scalability. The sort of flexibility that virtualization provides is critical to CyDesign product offerings, particularly for the modeling simulation and verification services. The platform will support bringing additional computation and storage services online to support specific simulation and verification runs.

Approved for public release; distribution unlimited.

4.4 Commercialization Approach

Under a subcontract to PARC, CyDesign Labs focused on the commercialization of the META tool chain. CyDesign Labs developed and delivered a commercialization plan for a mass-market tool chain based on the META / META-II research results. CyDesign Labs intends to commercialize the META tool chain as a web-based tool suite for model-based design and system engineering. The tool suite would target the design, modeling, and verification of complex cyber-electromechanical systems and products. The tool suite would be commercialized as a "mass market" tool suite at a price point that will enable widespread adoption and use.

The core mass-market tool suite is referred to as the CyDesign Studio. CyDesign Studio would consist of four building blocks:

- A collection of open source design tools, libraries, and capabilities developed under the DARPA Adaptive Vehicle Make (AVM) Program;
- Proprietary design and analysis tools for professional design engineers in certain key markets;
- An integration layer that allows seamless interoperation among the elements of the tool suite and legacy PLM tools, and provides social networking support for the CyDesign Studio user community;
- Vertically-integrated applications targeting selected industries and markets.

CyDesign Studio would be designed and deployed as a Software-as-a-Service (SaaS) product. The base tool suite will be deployed on a public cloud infrastructure such as Amazon's EC2 service. Through the public cloud deployment, the software will be available to anyone through a monthly subscription model. For applications where intellectual property protection is critical (e.g., ITAR restrictions or trade secrets), it will be possible to deploy the same infrastructure on an ITAR-restricted cloud infrastructure (e.g., Amazon's GovCloud) or on a private cloud behind organizational firewalls.

4.5 Architecture Design

PARC tasked CyDesign Labs to focus on the architecture design for the META tool chain. As a subcontractor to PARC, CyDesign Labs developed and delivered an architecture specification document for a mass-market tool chain based on the META / META-II research results. A summary of the architecture design approach is provided below.

CyDesign Studio will be a cloud-based platform for doing model-based design and analysis of complex cyber-electromechanical systems. The platform has two major user-facing tool sets - the Requirements Management Tool Set and the Trade Space Modeling Tool Set. Supporting the user facing tool sets are the CyDesign Forge and CyDesign Engines.

The platform users would access the Requirements Management Tool Set and the Trade Space Modeling Tool Set using an HTML5-capable browser. The platform users would not be required to install any desktop applications or databases.

The CyDesign Forge and CyDesign Engines will not be accessed directly by platform users. The users would access one of the tool sets (Requirements Management or Trade Space

Approved for public release; distribution unlimited.

Modeling). The tool sets access the CyDesign Forge and CyDesign Engine as needed through web service calls. The tool sets are a classic web application layer over a core platform layer (CyDesign Forge and CyDesign Engines).

The CyDesign Engines would run asynchronously with the platform users' sessions. Request to the CyDesign Engines will be queued and executed as the engine resource become available. Some of the Engine activities may require time-consuming processes compared to a normal user web session (such as simulations). The CyDesign Engines would allow the users to continue with other activities in an asynchronous fashion and notify the platform users when the engines have finished the tasks. At that time, the user would go back to the tool set and view the output from the engine.

The CyDesign Studio cloud-based solution would be deployable to both public and private clouds. For private clouds, especially secure clouds, the solution provider would not be required to deploy or run the solution. CyDesign development process of daily builds and deployments will regularly produce QA-approved builds for system administrators of private clouds to retrieve and install on their clouds.

The CyDesign cloud-based solution will utilize open source tools when possible. The solution would run on Linux servers. The tool set web applications would be written in Python using open source libraries or free development tools when possible. The forge would be based on Allura. The CyDesign Engines would be developed in Python. The simulation engine would also have the ability to process/compile C code files that are generated from Modelica models or using a Matlab compiler.

CyDesign Studio will be developed and deployed in stages. The solution provider will incrementally roll out functionality and receive user feedback on the deployed functionality. The functional releases would build upon each other and incorporate lessons learned from user feedback on previous releases. The rapid release and feedback cycle would allow the solution provider to make necessary improvements to previous release functionality while continuing to release new functionality.

4.6 Intellectual Property Analysis

As a subcontractor to PARC, CyDesign Labs developed and delivered an IP report that covered the IP rights and restrictions applicable to each candidate implementation for each tool required in the architecture. A summary of the IP report is provided below.

The CyDesign Studio platform would utilize several open-source platform tools and technologies. These tools and technologies are necessary to design, develop, deploy, and operate a scalable web-based application. In other words, the platform tools and technologies constitute the infrastructure upon which the business application (the mass-market design tool suite) will be built. These tools and technologies include the Ubuntu operating system, Allura software forge platform, Python scripting language, Java language, MongoDB and PostgreSQL databases, and various user interface libraries. All of these tools are available as free and open source, and none of these tools are subject to "viral" licenses that would require the customer code to be licensed under the same license. A list of the platform technologies and tools is provided in Table 2.

Approved for public release; distribution unlimited.

Technology	**Role**	**Licensor**	**License**	**Notes**
Ubuntu	Operating system	Canonical Group Ltd (UK)	various FOSS	Will use well-defined interfaces; no risk of contamination
Allura	Software forge	SourgeForge.net	Apache v2	Also used by GATech and Vanderbilt on VehicleForge.mil
Python	Scripting language	Python Software Foundation	Custom	GPL compatible, but not viral
Java	Programming language	Oracle	Custom	Not viral
MongoDB	Non-relational database	10gen	AGPL v3	GPL does not contaminate applications
PostgreSQL	Relational database	PostgreSQL Global Development Group	PostgreSQL License	Similar to MIT
Google Web Toolkit	Rich web application development	Google	Apache v2	

Table 2. Platform technologies intended for use in CyDesign Studio

CyDesign Studio would also include several tools and technologies tools are developed under the META, META-II, and META-X programs. These technologies include CyPhyML, PRISMATIC, QRM, PCC, Relational Abstractions, and Semantic Interoperability tools. All of these tools are available under a DARPA AVM open source license. Table 3 summarizes the META family tools intended for use in CyDesign Studio.

Approved for public release; distribution unlimited.

Technology	Role	Licensor	License	Notes
CyPhyML	metamodeling convention	Vanderbilt University	DARPA AVM	Will not use directly
PRISMATIC	Functional verification	Oxford University	DARPA AVM	Not planning to integrate at this time; will not be maintained as FOSS by Oxford
QRM	Safety verification	PARC	DARPA AVM	Not planning to integrate at this time
PCC	Performance verification	Oregon State University	DARPA AVM	
Relational Abstractions	Functional verification	SRI	DARPA AVM	Not planning to integrate at this time
Semantic Interoperability	Model translation	Vanderbilt University and Intentional Software	DARPA AVM	

Table 3. META tools and technologies intended for use in CyDesign Studio

Finally, CyDesign Studio may include various third party tools for additional functionality outside the scope of the META program family. Licenses for these tools will be negotiated as necessary.

Approved for public release; distribution unlimited.

5.0 CONCLUSIONS

During the 12-month base period of the META-II program, a team led by PARC has developed a model-based system-engineering framework that enables architectural analysis of complex systems during the conceptual design phase. Using this framework, design teams are able to systematically explore architectural design decisions during the early stage of system development prior to the selection of specific components. The analysis performed at this earliest stage of design facilitates the development of more robust and reliable system architectures. A final report summarizing this work was submitted at the end of the original period of performance.

The META-II contract was extended effective November 10, 2011 to study the commercial viability of the design tool chain being developed under the META and META-II programs. PARC partnered with CyDesign Labs and Red House Consulting in order to complete the new statement of work. The PARC team studied and analyzed the market opportunities for a commercial tool chain based on META tools and confirmed that there is a viable market opportunity. The PARC team then talked to a variety of potential customers and industry analysts, defined an architecture for the proposed commercial tool chain, and studied the IP and licensing requirements for the tool chain. Detailed findings were provided in a series of deliverables. The findings are summarized in this final report for the project.

Approved for public release; distribution unlimited.

6.0 REFERENCES

1. Kurtoglu, T., Bunus, P., and de Kleer, J., "Simulation-Based Design of Aircraft Electrical Power Systems," presented at the 8th International Modelica Conference 2011, Dresden, Germany, March 20-22, 2011.

Approved for public release; distribution unlimited.

APPENDIX A: PROJECT TEAM

Palo Alto Research Center (PARC)

Walter Johnson

Dr. Walter Johnson is Vice President and Director of the Intelligent Systems Laboratory research organization at PARC, a Xerox company. Focusing on analytics and modeling across a broad range of domains, the organization's researchers create social software to enhance collaboration and social cognition; model cyberphysical systems to plan, optimize, diagnose, and control complex processes in domains from manufacturing to energy management; and engage in agent-based modeling and simulation of complex work environments to improve processes in which humans and information systems are highly interdependent.

A former scientist in PARC's groundbreaking Human-Computer Interaction group, Johnson specialized in intelligent interfaces for mobile and ubiquitous computing applications. His work on a paper user-interface for document processing systems led to a special enterprise-level division being created to capitalize on this competency. Johnson also worked on a tablet computer startup at Silicon Graphics, and on portable document readers at PARC spinout Uppercase, Inc., which was acquired by Microsoft in 2000. He served as VP of Strategic Operations at incubator company 12 Entrepreneuring and, most recently, as SVP of Operations at real-time web-based news platform Skygrid.

Dr. Johnson obtained his Ph.D. in Cognitive Psychology from the University of Pittsburgh, and B.A. and B.S. degrees at the University of Arizona. Johnson has 14 patents.

Tolga Kurtoglu

Dr. Tolga Kurtoglu is Principal Investigator for the PARC META-II project and area manager of the Automation for Engineered Systems (AES) group at PARC. His research focuses on the design and development of complex systems, design theory and methodology with a specialization in conceptual design, design automation and optimization, and artificial intelligence in design. He conducts research in the areas of development of prognostic and health management technologies, model-based diagnosis, automated reasoning, systems engineering, and risk and reliability-based design. Dr. Kurtoglu has published over 50 articles and papers in various journals and conferences and is an active member of ASME, AIAA, AAAI, ASEE, Design Society, and the Prognostics and Health Management Society. Prior to his work with PARC, he worked as a researcher at NASA Ames Research Center and as a systems design engineer and lead at Dell Corporation.

Jonathan Propp

Mr. Propp is a Principal at RedHouse Consulting. He is a leading expert in the field of new product development. As a principal in Red House, he consults to technology firms throughout the Bay Area. He currently teaches OMIS 390, "New Product Development" in the Leavey School of Business at Santa Clara University. He is a certified New Product

Approved for public release; distribution unlimited.

Development Professional (NPDP) and a former board member of the Northern California chapter of the Product Development Management Association (PDMA).

His 23 years of experience in Silicon Valley includes companies such as Hewlett-Packard, Acuson, Mitsubishi Electronics, and Sun Microsystems Mr. Propp is a graduate of Harvard College and the Yale School of Management..

CyDesign Labs

Serdar Uckun

Dr. Serdar Uckun is the Principal Investigator for the CyDesign team under the PARC META-II project. He is the Founder and CEO of CyDesign Labs, Inc. Prior to founding CyDesign Labs in 2011, he was a Principal Scientist at PARC. Prior to PARC, he was at NASA Ames Research Center where he led the largest organization in the government focusing on prognostics and health management (PHM) research. Earlier, he served as Director of the Research Institute for Advanced Computer Science (RIACS), Director of Advanced Technology at Blue Pumpkin Software, and Assistant Director of Rockwell Science Center - Palo Alto Laboratory. Dr. Uckun has graduate degrees in Medicine and Biomedical Engineering, and he has completed post-doctoral studies in Computer Science at Stanford. His technical interests include diagnosis, prognostics, and optimization. He served as Associate Editor of the Artificial Intelligence in Medicine Journal and the General Chair of the 2008 International Conference on PHM. He is an Associate Editor of the International Journal on PHM. Additionally, he is founder and President of the PHM Society, a non-profit professional organization. He holds fourteen U.S. patents.

William S. Schaefer IV

Bill Schaefer is the Vice President of Engineering for CyDesign Labs. Before joining CyDesign, Bill was the VP of Engineering at Care2, the largest online community for healthy and green living. Bill has over 20 years designing, deploying and maintaining state-of-the-art distributed systems and content management solutions. He is a recognized expert in online advertising, global infrastructure and scalable systems. Bill has held executive positions at CyDesign, LLNL, JHU/APL, Revcube Media and the International Olympic Committee. Mr. Schaefer has an M.S.E.E.. from University of California at Irvine, Irvine, CA and a B.S. in Mathematics & Computer Science from California State University Stanislaus, Turlock, CA.

Approved for public release; distribution unlimited.

LIST OF ACRONYMS AND ABBREVIATIONS

ACRONYM	DESCRIPTION
A&D	Aerospace and Defense
AEC	Architecture, Engineering, and Construction
ALM	Application Lifecycle Management
CAD	Computer-Aided Design
CASE	Computer-Aided Software Engineering
DARPA	Defense Advanced Research Projects Agency
DDTE	Design, development, test, and evaluation
EDA	Electronic Design Automation
IP	Intellectual property
MCAD	Mechanical Computer-Aided Design
NC	Numerical Control
PARC	Palo Alto Research Center
PDM	Product Data Management
PLM	Product Lifecycle Management
PRD	Product Requirements Document
SaaS	Software-as-a-Service

Approved for public release; distribution unlimited.